Interim Report
Fingerprint Authentication in an Embedded System

February 16, 2007

Wade Milton 0284985
Jay Hilliard 0236769
Breanne Stewart 0216185

A.I.D
Analysis and Intelligent Design

University of Guelph
School of Engineering

Analysis and Intelligent Design
1428 Elm Street
Soeville, ON
N1L 2H0
(519) 767-0115

February 16, 2007
Project No. 07-01

S. Areibi
School of Engineering
University of Guelph
Guelph, ON,
N1G 2W1

Subject: Fingerprint Based User Authentication

Enclosed please find a copy of *Analysis and Intelligent Design's* interim report for the embedded fingerprint based user authentication system. We have currently looked at the 3 different parts of supporting efficient fingerprint based user authentication in an embedded system and 2 different hardware options. We are going to put more emphasis on image processing and fingerprint classification than on authentication and the DSP starter kit and fingerprint development kit have been ordered as the hardware component at $796.51. A final report on the chosen design will be delivered on April 9th, with a poster presentation on April 5th.

Sincerely,

Wade Milton

Jay Hilliard

Breanne Stewart

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Problem Statement

The focus of this project is to look at the problems surrounding fingerprint-based user authentication in an embedded system. Biometric authentication is the use of physiological characteristics such as a fingerprint, hand shape, face map, voice, or iris to determine the identification of the user [1]. This type of identification is more reliable in comparison to traditional verification methods such as possession of an object like a key or swipe card, or the knowledge of a password or login, because the person has to be physically present at the time of identification [2]. Reliable personal identification is important in everyday transactions ranging from petty ATM withdrawals to high security building access. Biometric identification could decrease billions of dollars lost every year to credit card fraud, welfare “double-dipping”, cellular bandwidth thieves, and ATM fraud by providing near irrefutable proof of identification.

1.2 Objectives

- Identify problems in fingerprint-based authentication in an embedded system; provide solutions in image processing, classification, and authentication.
- Compare different fingerprint specific algorithms and programs
- Give reasons why one is better than another: security, accuracy, user friendly, and speed etc.
- Write programs from others which we think would work better for fingerprint feature extraction, enhancement, matching, and classification.
- Final product will be something that embodies the best program on our obtained DSP (digital signal processing), microcontroller, or any computer.

2. Background

2.1 Fingerprint Biometrics

The fingerprint is the most widely used biometric trait. All fingerprints are believed to be unique to each person and finger; even twins do not have the same fingerprints [1]. Fingerprint technology is the most developed technology in biometric recognition [3], and is legitimate proof of evidence in courts of law all over the world [2].

Fingerprint recognition has been used for a significant amount of time. The “Henry system” was developed in the early 1800’s by Edward Henry to classify and identify fingerprints based on the ridge configurations and was revamped by the FBI in the early 1900’s [3]. The categories are based on the global patterns of the ridges and valleys. The human fingerprint can have many different ridge patterns. The six general classifications are: the arch, tented arch, the right loop, the left loop, the whorl and the twin whorl as seen in Figure 1. Loops are the most common pattern found making up nearly 2/3 of all fingerprints, whorls making up almost 1/3 of all fingerprints, and arches making up the last 5-10% [4]. There is also an accidental category but it is very rare and covers the fingerprints that do not clearly fall under any of the other categories.

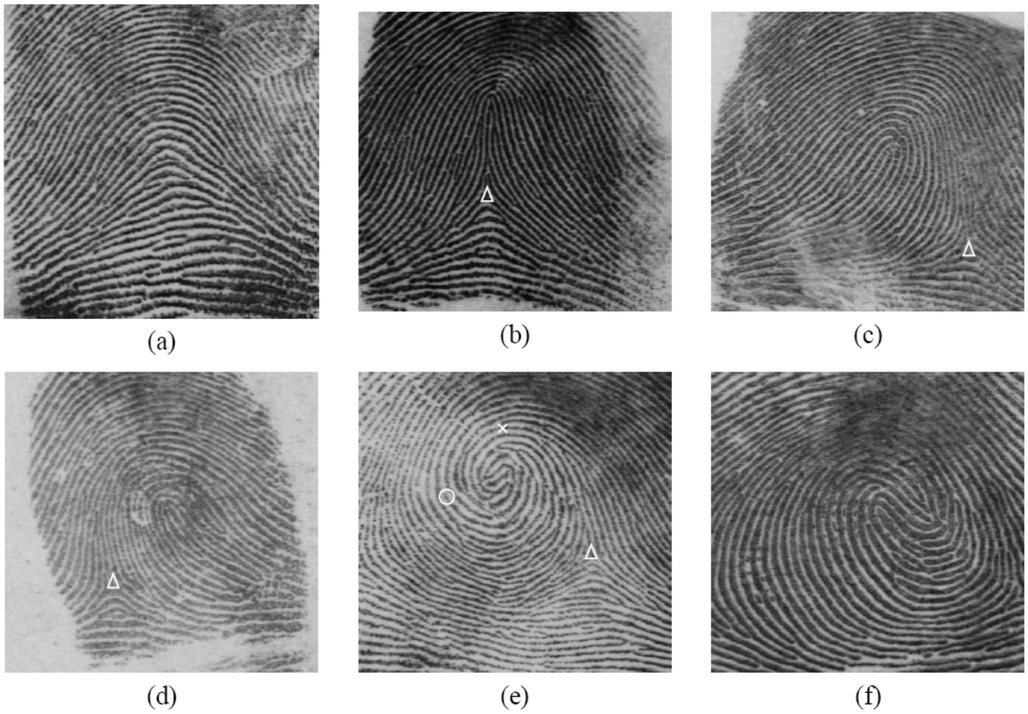


Figure 1: Different fingerprint patterns. (a) arch, (b) tented arch, (c) right loop, (d) left loop, (e) whorl and (f) twin loop [2]

2.2 Fingerprint Analysis

The minutiae-based fingerprint matching is very popular because it is considered to be the most discriminating feature on the finger. Minutiae-based fingerprint analysis involves matching the local discontinuities or minutiae of the fingerprint. Discontinuities in a fingerprint include terminations or ridge endings and the bifurcations where ridges fork or diverge [5]. The information for a fingerprint is then stored as a point pattern of minutiae instead of a complete image of a fingerprint [6]. It is also simpler compared to other forms of fingerprint matching such as ridge-pattern based or complete image based and is fast and has a small template [2].

There are 4 main components to fingerprint-based user authentication: user interface, image processing, classification, and authentication. The user interface is where a fingerprint sensor is used to read the finger and send the image to be analyzed. There are two basic types of fingerprint sensors: swipe and area sensors. As implied, the swipe sensor takes an image of the fingerprint while a finger is swiped across it and the area sensor takes an image as the finger is pressed on the sensor. In both cases, the resulting data that represents the fingerprint image is stored in a matrix of pixels to show the characteristics of the fingerprint. Next there is image processing were the original image is converted into a form that can be used to extract the minutiae points. This includes passing the image through a series of filters to make the image clearer and more concise. Following this is classification where the fingerprint is distinguished as part of a smaller group of fingerprint types so that it is not compared to every fingerprint in the database. The authentication stage validates the identity of the individual by extracting the pattern of minutiae from the fingerprint and subjecting it to a matching algorithm in an effort to match it against one of the templates stored in the system database.

2.2.1 Evaluation Techniques

Fingerprints from the same finger will be slightly different every time they are scanned for a number of reasons so there will not always going to be a perfect match for the same fingerprint. There is random noise, skin condition at the time of scanning (e.g., dry, sweaty, dirty, etc.), as well as the pressure and position of the finger. To evaluate the accuracy of the algorithm for minutiae matching, a genuine score and an impostor score can be generated. A genuine score is made by comparing the fingerprint minutiae from two separate readings of the same finger, and the impostor scores by comparing the fingerprint minutiae from reading two separate fingers [1]. Using the percentage from the genuine score gives the Genuine Accept Rate (GAR), and using the percentage from the impostor score gives the False Accept Rate (FAR). The GAR and FAR can then be plotted against each other at various operating or threshold values (T) to generate the Receiver Operating Characteristic graph as seen in Figure 2.

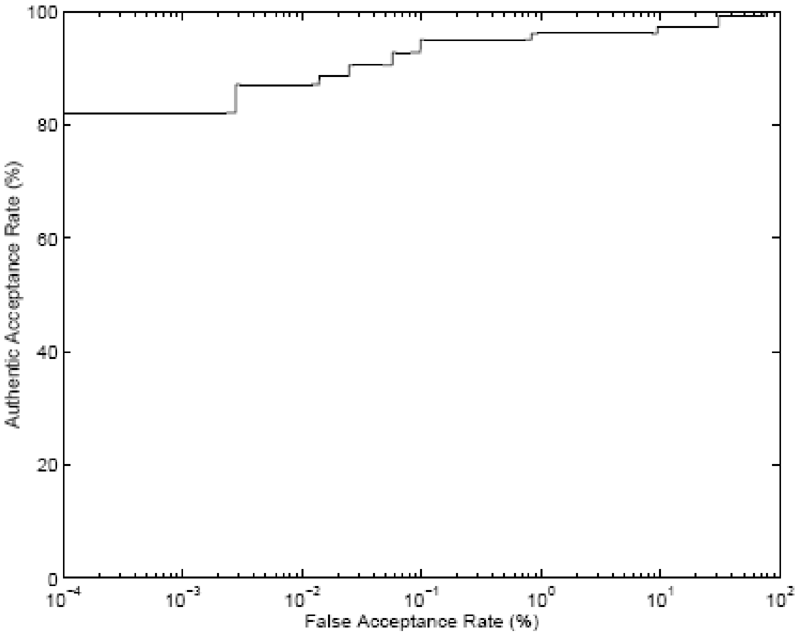


Figure 2: Receiver Operating Characteristic. [2]

The graph must be represented as a percentage and therefore must start at (0,0) and end at (1,1), or (100,100) as a percentage [7]. This can then be used to compare different methods implemented at any stage and their influence on the effectiveness of the system.

2.3 Constraints

- The processor must be secure from interference and tampering that could lead to unauthorized entry.
- The sensor should be able to withstand a minimum of 500,000 samples per year.
- The system must have a minimum accuracy of 99.99%.
- The system must not allow unauthorized entry.
- The system must not generate false positive matches.

2.4 Criteria

- Minimize the cost of the design.
- Minimize the size for compatibility and mobility.

- Maximize the simplicity of the user interface.
- Maximize the speed of authentication.
- Provide usable solutions to problems for fingerprint-based authentication in an embedded system.
- Algorithms should be as easy to understand as possible and upgradeable.

2.5 Assumptions

- Assume that a finger is being scanned from a real person.
- The development kit will be available in a suitable amount of time to implement and test programs.
- Power supply will be available on all sites that it might be used.

3. Design

3.1 Design I

Image Pre-Processing

This step is the most processor intensive and has the largest impact on subsequent steps. This is where an image or grey-scale representation of a fingerprint is taken and processed through a series of filters in order to create a more reliable and concise picture to be compared to database values. Many of the filters involved require multiplication and/or division, usually multi-cycle operations, of every pixel or a subset of pixel groups. For example, the mean filter requires the average of the eight surrounding pixels to apply to the center one, thus 9 complex operations for every pixel. Most modern scanners have a resolution of at least either 128 or 256 pixels square resulting in about 590,000 complex operations when applying the mean filter on an image. This step is also the most resource intensive since an image must be stored pixel by pixel regardless of redundant or similar image patterns within the fingerprint. Some filters also require additional preprocessed information in the form of overlaying masks creating 2 or more data structures of equal size to the image.

Since the scope of this section is so great with many different permutations that could be tested, we suggest that the bulk of this investigation continue specifically within this realm. In addition, any increased performance or image clarity will have an immediate and prominent effect on the latter steps.

3.2 Design II

Pattern Classification

Once an image has been processed to create a clearer picture, patterns can be extracted and classified. This helps in reducing computational time in the authentication stage by testing only certain “bins” of classes, such as whorls or arches. This will be the least computationally intensive stage since it will only involve pattern recognition and will not require complex calculations. Since this is the next stage in development we propose that a brief technical analysis of the different possible classifications be made, but that further development and implementation be postponed for future endeavors. Time permitting as much work as possible can be attempted, but results should not be expected to be final or conclusive.

3.3 Design III

Authentication

The final step in allowing a user restricted access to a resource is to ensure that the requesting user has sufficient security rights. This involves comparing the points of interest gathered by the previous steps to a database of authorized users. Depending on which algorithm is chosen, this stage can become computationally heavy but will not be as resource intensive as the first step. To accurately match a supplied print to database values the distances between various points must be calculated. To increase accuracy the unit vector of each minutia may also be used in calculating point relations, which adds to the complexity of the equations. The unit vector of a point is the apparent direction which the feature is pointing based on some static criteria. Some methods introduce matrices to solve these systems, but either way multiplication or division will be required, but on a much smaller data set than the filters. Since there are many methods which could be investigated and compared, we suggest that this stage be researched and implemented thoroughly on its own. This stage must be the most discriminate since unauthorized access to a restricted resource cannot be tolerated, and thus an exhaustive study would be necessary.

3.4 Methodology

3.4.1 Analysis Techniques

A review of the literature on dealing with fingerprint analysis shows that there are three main steps that are required to implement fingerprint authentication. The first step involves pre-processing of the fingerprint information so that information can be reliably extracted from the fingerprint data. The next step is to classify the fingerprint into one of several sub-categories. By further classifying fingerprints they do not need to be compared with all the reference fingerprints but only those in its category. The last step is to try and reliably match the fingerprint to one of the stored reference prints. Within these main steps there is a variety of methods but each one attempts to produce a similar result. Ideally this is an enhanced fingerprint that will provide valid information that allows for it to be matched to previously sampled information.

It is obvious from our literature review centered on fingerprint analysis and early attempts to implement some the common algorithms suggested within articles that the complete task of fingerprint authentication is far from trivial. For this reason, our project will concentrate on the pre-processing of the grey-scale fingerprint image and to assign fingerprints to different classes. Fingerprint matching techniques will not be directly addressed.

The first step in any fingerprint authentication system is to take a sample of the fingerprint. This is usually done through the use of a sensor but could be done with manual techniques. The important detail about sampling a fingerprint is that the information must be converted to a form that can be manipulated using a digital system. This means that regardless of the source from which the fingerprint is taken, the end result is a matrix of pixels that represent the grey-scale ridge and valley structure of the fingerprint.

The major issue that stems from taking fingerprint samples is the quality of the information. The clarity of the fingerprint will directly affect the system's ability to match a fingerprint sample which is the reason why the image needs to be processed before matching can be attempted. Most of the articles reviewed suggest a basic methodology for image pre-processing which is shown below in Figure 3.

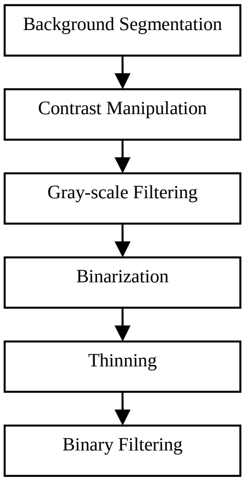


Figure 3: Flow chart for Image pre-processing.

3.4.2 Background Segmentation

Fingerprint images may have background information that is not be part of the fingerprint. The process where the background information is removed is referred to as background segmentation and may be required as the first step in the pre-processing of the fingerprint. The need for background segmentation will depend greatly on the individual methods used to create the digital representation of the fingerprint image. This process is usually done by dividing the fingerprint image into square blocks of eight or sixteen pixels. For the purpose of this document, a block will be considered as a square sub-sample from the image matrix. The variance in the grey-levels of the pixels in a block is then compared to the variance of the entire image. Any block that varies beyond some threshold will be considered to be invalid information pertaining to the fingerprint. Functions that perform background segmentation have been implemented. This is a fairly easy task but the problem is to correctly choose what threshold will be used to properly separate the background from the fingerprint image. So far trial and error has been used to determine this threshold value.

3.4.3 Contrast Manipulation

The quality of fingerprints will almost never be consistent. In fact, most will be fairly poor. For this reason, fingerprints need to be enhanced to improve the quality of results. To improve the clarity of the fingerprint some sort of filtering is required. To aid in the image filtering, the grey-scale levels of the fingerprint are usually manipulated to help enhance the effects of filtration. Two common methods of contrast manipulation are normalization and histogram equalization. Normalization standardizes the grey-level intensities of the pixels in the overall matrix of pixels that represent the fingerprint. One method used to accomplish this uses the mean and variance of the pixel intensities in the image. You specify a desired mean and variance and shift the actual mean and variance of the fingerprint to better match these values. This information is then used to shift the actual pixel intensities proportional to a manually specified mean and variance [8].

Another method suggested to enhance the contrast of an image is to use histogram equalization [9]. This is being looked into further.

After this stage, the ridge and valley structure is not changed but the variation of the grey levels or the pixels is reduced to aid with the future steps used to enhance the fingerprint.

3.4.4 Grey-scale Filtering

The majority of the articles in the last ten years strongly reference the article by Hong et al. that suggests fingerprint enhancement based on filtering the image using a Gabor filter. Early efforts were focused towards trying to implement this suggested algorithm that is shown below in Figure 4 [8].

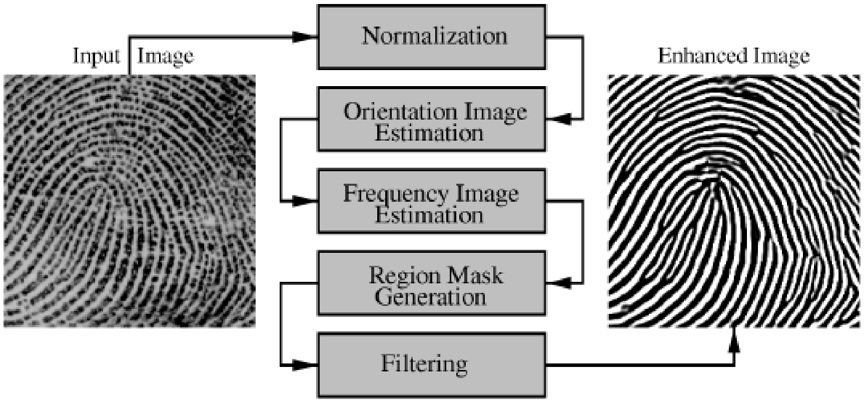


Figure 4: Flow chart for a Gabor filter [8].

The main issue with this technique is that the Gabor filter requires an estimation of the block orientation around each pixel and an estimation of each block’s frequency. This information is then used create a complicated filter mask from the Gabor 2-D symmetric filter equation. Once the mask is calculated, it is convolved with each pixel to produce a filtered image for that block. This process is then repeated for every pixel and the associated block around it. These three steps require complicated algorithms that are computationally expensive and for this reason the Gabor filter will not be pursued further.

Greenberg et al. in "*Fingerprint Image Enhancement using Filtering Techniques*" suggests a method that does not require the use of a Gabor filter. This is the method that will now be pursued with respect to the pre-processing of fingerprint images. A block diagram of the Greenberg et al. process is shown below in Figure 5 [9].

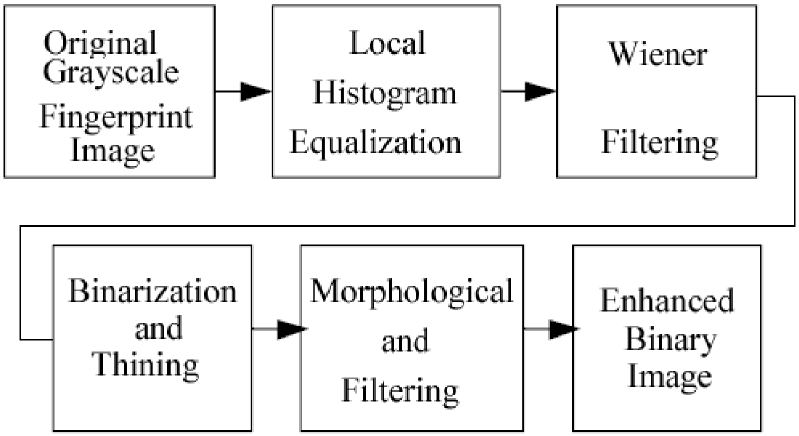

Original Grayscale Fingerprint Image
Local Histogram Equalization
Wiener Filtering
Binarization and Thining
Morphological and Filtering
Enhanced Binary Image

Figure 5: Block diagram for Wiener filtering method [9].

As the block diagram depicts, this method uses a Wiener filter instead of the Gabor filter and the article claims it is much easier and less computationally expensive than the Gabor filter method.

3.4.5 Binarization

Binarization is an easy to implement process that just compares each pixel to some threshold value and then changes its value to either pure white (0x00) or pure black (0xFF). The threshold used is usually either the global mean or a local block mean. This has been implemented using a local block mean.

3.4.6 Thinning

When a fingerprint is sampled it can often be slightly smeared or affected by pressure differences between samples. Both of these issues will cause the ridge structure width to vary. Thinning reduces the ridge structure of the fingerprint to a skeleton structure that is only one pixel wide and helps remove these issues. Thinning also reduces the complexity of matching fingerprints by making the internal structure easier to analyze. Greenberg et al. does not explicitly state which thinning algorithm they have implemented, so one from the article by Zhou et al. [9] has been chosen since it is referenced by many of the articles on fingerprint analysis. This algorithm has been implemented but some more testing is required. Our implementation does work but has been found that it requires multiple passes instead of a single pass as touted within the article.

3.4.7 Binary Filtering

Once again Greenberg et al. do not explicitly state the binary filtering algorithm that they use but do state that this is fairly mechanical process of manually finding and removing ridge structures that probably do not belong and by filling in gaps in ridges that do not belong. This stage has not yet been implemented.

3.4.8 Hardware Costs

Table 1: Cost breakdown of hardware options.

Items	Cost
Hardware Option 1	
Fingerprint Sensor Interfacing Device	$304.91
DSP Board	$491.60
Total	$796.51
Hardware Option 2	
Fingerprint Sensor	$5.00
Microcontroller	$20.00
PCB Fabrication & Assembly	$110.00
Total	$135.00

These 2 options were explained in the proposal handed in January 15, 2007.

3.5 Design Plan

The final design will be a mixture of the three stated above with emphasis put on the first two designs. This was chosen because image processing is the first step to authentication and without a good image there cannot be an accurate authorization. A brief technical analysis of the different possible classifications will also be completed since it is not as computationally intensive as the other options. The authentication will be investigated but will be saved for future groups to work on.

Hardware option 1 has been chosen because it will be the most accurate and reliable of the two hardware options. Even though the price is much more than the second option, funding was provided to cover the cost of the entire development kit including the DSP and fingerprint development kit. See the appendix for a breakdown of the funding.

Further progress will be made to implement the Wiener filtering method and the other steps in image processing. As well, a review of the different types of fingerprint classification will be thoroughly looked into and compared.

3.5.1 Time Schedule

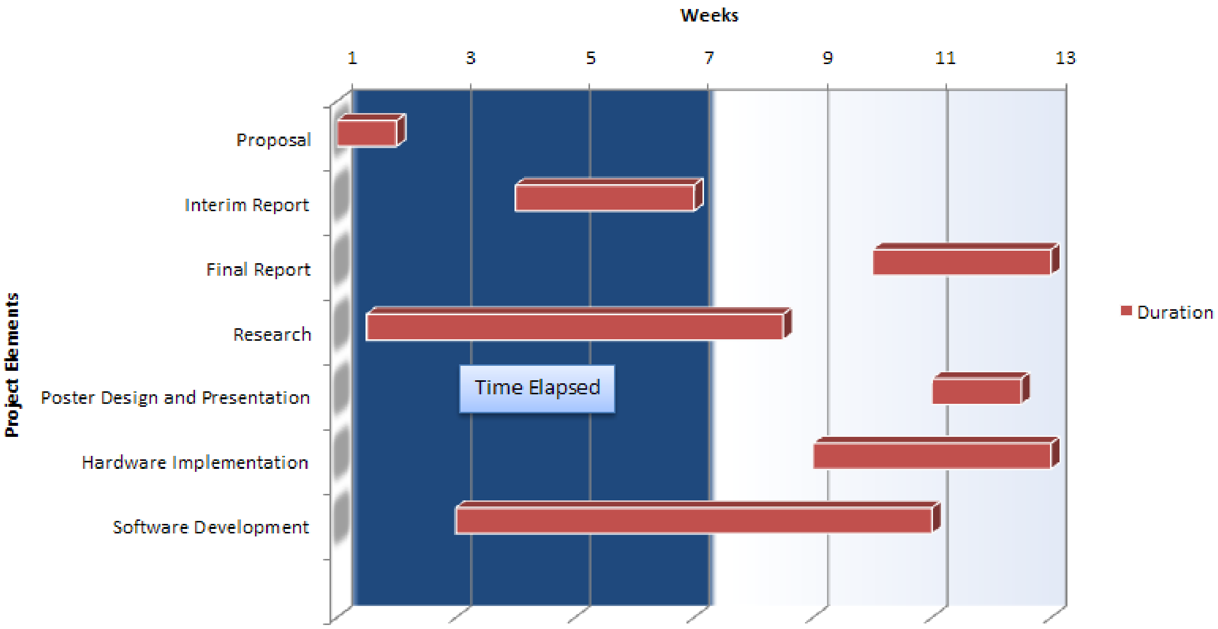


Figure 6: Gantt chart.

4.5.2 Deliverables

Interim Report ………………………………………………………….February 16, 2007
Final Design Report………………………………………………………… April 9, 2007
Poster Presentation……………………………………………………….. April 5, 2007

4. Conclusions and Recommendations

This project is focusing on the problems with fingerprint-based authentication in an embedded system. There are three main areas to look at in fingerprint-based authentication: image processing, classification and authentication. To fully look at all the problems we think it is best to actually attempt to write the programs needed to go from reading the fingerprint in from the sensor to classifying the fingerprint. This way we will experience the problems first hand and be able to best describe what they are and suggest or develop a solution. There will be more emphasis put on image processing and classification in this project.

The DSP kit and fingerprint sensor have been purchased with the money that has been provided but this may be for the use of future projects more than this one for the purpose of a final demonstration of all amalgamated results.

5. Reference

[1] A. Jain, “Fingerprint matching”, http://www.pims.math.ca/industrial/2002/mitacs-agm/jain/, January 2007.

[2] A. Jain and S. Pankanti, “Fingerprint Classification and Matching”, http://www.research.ibm.com/ecvg/pubs/sharat-handbook.pdf, January 2007.

[3] R. Bolle, J Connell, S. Pankanti, N. Ratha and A. Senior, “Guide to Biometrics” New York: Springer, 2004.

[4] “Fingerprint Identification”, http://webfea-lb.fea.aub.edu.lb/dsaf/labs/projectv1.1.pdf, January 2007.

[5] M. Aladjem, I. Dimitrov, S. Greenberg and D. Kogan, “Fingerprint Image Enhancement using Filtering Techniques,” Pattern Recognition, 2000. Proceedings. 15th International Conference, Vol. 3, pp. 322-325, 2000.

[6] X. Jiang, and W. Yua, “Fingerprint Minutiae Matching Based on the Local And Global Structures”, 15th International Conference on Pattern Recognition (ICPR'00). Vol.2. 2000. pp. 1038-1401.

[7] W. Langdon, “Receiver Operating Characteristics (ROC)”, http://www.cs.ucl.ac.uk/staff/W.Langdon/roc/, February 2007.

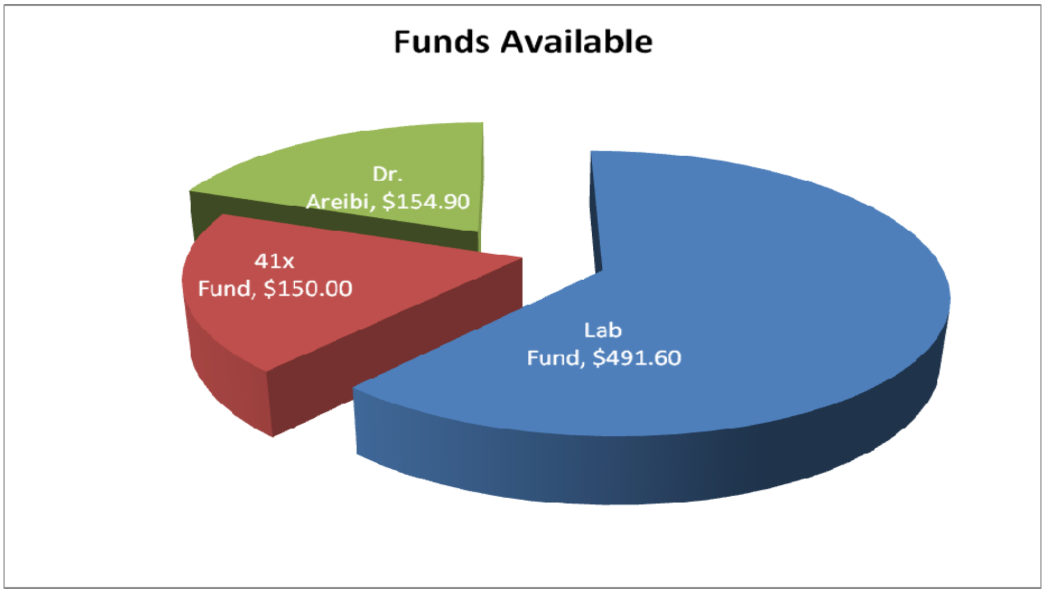
[8] L. Hong, Y Wan, and A. Jain, “Fingerprint Image Enhancement: Algorithm and Performance Evaluation,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 20, no.8,pp.777-789, 1998

[9] S. Greenberg, M. Aladjem, D. Kogan, and I. Dimitrov, “Fingerprint image enhancement using filtering techniques”, Pattern Recognition, Proceedings. 15th International Conference on, vol. 3, pp. 322-325, 2000.

[10] R. Zhou, C. Quek, and G.S. Ng, A novel single-pass thinning algorithm and an effective set of performance criteria *Pattern Recognition Letters*, 16(12), 1267-1275, 1995

6. Appendix

Funding Breakdown:


Funds Available
Dr. Areibi, $154.90
41x Fund, $150.00
Lab Fund, $491.60